

Status	<b>of 26.12.2008 - has terminated</b>
<b>(11)</b> Number of the patent document	<b>2091983</b>
<b>(13)</b> Kind of document	<b>C1</b>
<b>(14)</b> Document date	<b>1997.09.27</b>
<b>(19)</b> Publishing country or organization	<b>RU</b>
<b>(21)</b> Application number registered	<b>93007865/09</b>
<b>(22)</b> Application filing date	<b>1993.02.09</b>
<b>(45)</b> Date	<b>1997.09.27</b>
<b>(516)</b> Edition of IPC	<b>6</b>
<b>(51)</b> Main classification IPC	<b>H04L9/00</b>
<b>(51)</b> Main classification IPC	<b>G06F12/16</b>
Title	<b>METHOD OF CODING OF BINARY INFORMATION AND DEVICE FOR ITS REALIZATION</b>
<b>(71)</b> Applicant information	<b>Chizhukhin Gennadij Nikolaevich</b>
<b>(72)</b> Inventor information	<b>Chizhukhin Gennadij Nikolaevich</b>
<b>(73)</b> Grantee (asignee) information	<b>Chizhukhin Gennadij Nikolaevich</b>

### **#2091983. Abstract**

FIELD: cryptography at arrangement of devices of commercial closed communication.

SUBSTANCE: an N-bit secret key is formed, with the aid of which a flow code is formed, summation being modulo 2 with an information text; the flow code is formed as K groups with N bits in each, where  $k \cdot N$  - length of the text being processed. The first group of the flow code is formed by raising the N-bit secret key to the n power to modulo P, and the second group of the flow code is formed by raising the N-bit code of the first group of the flow code to the n power to modulo P, where n - number of least-significant bits of the secret key with  $1 < n < N < P-1$ , and each subsequent i group of the flow code, where  $i=3,4,\dots,k$ , is formed by raising the n-bit code of the i-1 group of the flow code to the m power to modulo P, where m - number of least-significant bits of the i-2 group of the flow code,  $m=n$ ; prior to taking a sum to modulo 2, in each group of the K groups of the formed flow code the bits are mixed in an accidental manner and memorized. The device for realization of the method uses unit 1 for raising to n power to modulo P, power register 2, secret key register 3, key group register 4, sequence bit mixing unit 5, first and second modulo 2 adders 6 and 7, key 8, control unit 9, serial- alternate registers 10<sub>1</sub>-10<sub>4</sub>, OR gate 11 and AND gates 12 12<sub>1</sub>-12<sub>3</sub>. EFFECT: enhanced safety of information in computer commercial communication systems. 2 cl, 1 dwg

